Security Advisory 2022-085

Type Confusion Vulnerability in Chrome Browser

December 5, 2022 — v1.0

TLP:CLEAR

History:

- *5/12/2022 — v1.0 – Initial publication*

Summary

On December 2, 2022, Google released a new version of its Chrome browser fixing a high-severity flaw, identified by `CVE-2022-4262` [1] that could allow a remote attacker to potentially exploit heap corruption via a crafted HTML page.

Google is aware of reports that an exploit for CVE-2022-4262 exists in the wild. It is highly recommended to apply the update.

Technical Details

The `CVE-2022-4262` is a type confusion in the V8 JavaScript engine. Type confusion vulnerabilities arise when a program allocates or initialises a resource such as a pointer, object, or variable using one type, but it later accesses that resource using a type that is incompatible with the original type [2], potentially allowing an attacker to perform out-of-bound memory access.

Google keeps the access to bug details and links restricted until a majority of users are updated with a fix.

Affected Products

- Google Chrome for Mac, Windows and Linux before version `108.0.5359.94`.

Recommendations

CERT-EU recommends updating to the latest version.

References

[1] https://chromereleases.googleblog.com/2022/12/stable-channel-update-for-desktop.html

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4262